The Application of SSL Protocol in Computer Network Communication

Tian Huan

Lanzhou Vocational Technical College, Gansu Lanzhou 730070, China

Abstract. Since nineties of last century , the world have feaced the Internet storm.From then on,network application have began to go into every aspect of our lives gradually. But the traditional Internet Protocol (TCP / IP) does not provide information transmission security mechanism.From the technical level, how to solve the problems of network information thefting, tampering, hacking attack have become a pressing matter of the moment of our science and technology workers. This paper is precisely based on this perspective. Through this views,we analyse and discuss the computer network communication protocol deeply. From the theoretical level, the SSL protocol is applied to the TCP protocol. From doing so,the problem of information transmission security that cannont be solved by traditional TCP/IP protocol will be solved successfully. At the last, an example of online bank specific will be discussed, the reaserch of this paper will be uesd in this example.

Keywords: TCP/IP, SSL;Signature, Information encryption.

1 Introduction

Since nineties of last century , the world have feaced the Internet storm.From then on,network application have began to go into every aspect of our lives gradually . With the remarkable achievements made at the same time, we also have to pay attention to an intensified phenomenon: of hacking in internet. What is the reason leading to the phenomenon of deterioration? This paper will discuss which factors lead to the occurrence of this phenomenon? At the same time, the corresponding technical means will be applied to correct this problem. At last, the latest research results applied to a sample unit specific description.

2 Basic Theory(TCP and SSL)

At present in the world computer network communication, we use the standard of TCP / IP[1] (Transmission Control Protocol / Internet protocol) protocol which was put forward by American Researchs. The protocol is designed for computer communication development application protocol, it through the hierarchical classification method, the complicated logic relationship into five distinct layers relationship. The five layers are: Application Layer, Transport Layer, Network Layer, Data Link Layer, Physical Layer. See chart below(Table 1):

Z. Du (Ed.): Intelligence Computation and Evolutionary Computation, AISC 180, pp. 779–783.
springerlink.com

Table 1. The hierarchical structure of TCP/IP protocol

Application Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

The TCP / IP protocol in the establishment of communication, which solve network congestion, processing network conflict has obvious advantages. But the agreement in the development stage, how to prevent the computer communication from hacking was not fully taken into account (also may not consider). So the agreement, not to the network security, information security for any given (from Table2.1 can be seen, the agreement of the five layer system structure, without any one layer according to the safety specific processing mechanisms). Through the computer network to transmit the information, are clear (unencrypted treated) transmission, and transmitted in the network without the corresponding information transmission tamper resistant, anti attack security validation. So through certain technical means, can be implemented easily steal each other's transmission information (all the final transmission data in the Table2.1 Application Layer), or for any party to transfer the information to distort, attack. How to solve the above problem, become the computer development, must solve the imminent problems.

In order to solve the above problems, especially the introduction of the NetScape SSL protocol[2] (Secure Socket Layer). The SSL protocol in TCP / IP protocol model of network layer and application layer (Network Layer) (Application Layer), which uses TCP to provide a reliable end-to-end security services, it ensures that the client / server communication between the not to be attacked, tapping, and always on the server for authentication, can also choose on the client side authentication. The SSL protocol also adopts the hierarchical method,, it also adopts a hierarchical classification method, the complicated logic relationship into four distinct layers relationship. This four layer respectively(Table 2):

Table 2. The hierarchical structure of SSL protocol

Application Layer
SSL Handshake Protocol Layer
SSL Record Protocol Layer
TCP layer

3 The Application of SSL Protocol in Computer Network Communication

Based on the traditional TCP / IP network communication information[3] without any encryption and authentication mechanism, we will apply the the SSL protocol which was introduced in section 2 to computer network transmission. Through respectively in client and server sides, SSL protocol is added to the TCP / IP layer and Application